Abstract

A compression method of digital signature by a simple procedure not requiring a huge amount of calculation, all the way being one-way, wherein a series of numerals a(k) of an arbitrary length is input and arranged in a matrix A(n x n) according to a predetermined arrangement procedure (step P01), next, an algebraic value taken as modulo 10 which is an addition value of respective digits in the line direction and row direction of the matrix A(n x n) is output as compressed numeral A'(n + n) (step P02), thereby, numerals of n digits of respective lines and rows are compressed to a single digit, and the matrix A(n x n) of n x n digits as the whole is compressed to a compressed numeral A'(n + n) of n + n digits in length and width, then, it is judged whether there is a remainder of the series of numerals a(k) to be input, and if there is none, the processing is terminated (step P03), and in case there is a remainder to be input, it is arranged in a matrix A(n x n) according to the same arrangement procedure as the step P01 taking the compressed numeral A'(n + n) output in the step P02 as the first input numeral, before returning to the step P01 (step P04); and in the step P01, the compressed numeral A'(n + n) and the remaining series of numerals a(k) input following the same are arranged in a matrix A(n x n) according to a similar arrangement procedure.